热工控制系统网络安全隐患及防护对策研究

李世龙　张　倩

大唐黑龙江发电有限公司哈尔滨第一热电厂　黑龙江　哈尔滨　150001

摘　要：热工控制系统是电力、石化等流程工业的核心神经，其网络安全直接关系到生产安全与能源命脉。本文深入剖析了热工控制系统在通信协议、操作系统、管理制度及供应链等方面存在的固有脆弱性，系统梳理了勒索软件感染、内部恶意运维等典型攻击场景。在此基础上，提出了涵盖网络架构隔离、边界防护、主机加固、纵深防御及全生命周期管理的系统化防护对策，并针对典型攻击场景给出了阻断路径与控制措施。构建适应工控系统特性的纵深防御体系，将安全理念深度融入系统全生命周期，是保障热工控制系统网络安全的核心路径。

关键词：热工控制系统；DCS；工业控制安全；网络安全

引言：热工控制系统以集散控制系统（DCS）为核心，对温度、压力、流量等热工参数进行实时监测与自动调节，是保障机组安全稳定运行的中枢。传统上，热工控制系统运行于封闭专网，依靠物理隔离实现安全。然而，随着“两化融合”深入推进，系统大量采用通用计算平台和标准通信协议，并与管理信息网频繁数据交换，封闭边界被打破后系统直接暴露于复杂网络环境中。近年来，全球针对电力关键基础设施的网络攻击频发，从“震网”病毒到勒索软件导致电厂停机，均表明传统以隔离为信条的安全理念已难以应对当前形势。亟须立足工控系统特殊性，研究制定系统性的网络安全防护对策。

1 热工控制系统网络架构与安全现状

1.1 系统组成与网络架构

热工控制系统采用分层分布式架构，自下而上划分为过程控制层、操作监控层和生产管理层。过程控制层由现场控制站、I/O 模件及智能设备组成，完成数据采集与闭环控制，通信网络多为专用实时网或工业以太网。操作监控层由操作员站、工程师站及数据服务器构成，实现集中监视与操作干预。生产管理层通过网关与上层信息系统互联，完成数据上传与指令下达。传统物理隔离下各层级仅内部通信，不接入外网。但随着信息化推进，操作监控层与管理信息网间设置了横向单向隔离装置，系统中越来越多采用标准 TCP/IP 协议设备，工控协议在开放网络上传输成为常态，攻击面显著扩大。

1.2 网络安全现状与典型威胁趋势

当前热工控制系统网络安全处于“被动防御”与“合规导向”的初级阶段，普遍存在“重功能安全、轻网络安全”的认知偏差。大量在役机组设计阶段未充分考虑网络安全，带病投运后整改难度极大。国内 DCS 系统网络安全审计中，中高风险项集中在补丁缺失、杀毒软件过期、弱口令、无账户锁定及操作审计缺失等方面[1]。威胁趋势上，攻击已从“炫耀式”入侵演变为以勒索和破坏为目的的“精准打击”，手段涵盖网络渗透、U 盘摆渡、供应链预置后门及社会工程学等。系统一旦被攻破，轻则参数篡改引发误动，重则机组停运甚至设备损坏，后果远超 IT 系统数据泄露，直接危害国家能源安全与公共安全。

2 热工控制系统网络安全的主要隐患

2.1 通信协议与网络架构的固有脆弱性

热工控制系统广泛采用的 Modbus/TCP、DNP3、IEC 60870-5-104、S7 通信等工业控制协议，设计之初以功能实现和实时性为核心，几乎未考虑安全机制，普遍缺乏身份认证、数据加密和完整性校验。攻击者接入网络后可通过协议解析工具捕获通信报文，实施流量分析、指令重放、参数篡改等攻击，如在 Modbus/TCP 通信中伪造写指令改变关键参数而操作员毫无察觉。另外，系统网络架构扁平化加剧了风险——过程控制网与管理信息网互联后，攻击面从单一管理终端扩散至全部现场控制站，横向移动路径被大幅缩短。

2.2 操作系统与通用软件的安全短板

当前主流 DCS 系统的工程师站和操作员站普遍采用 Windows 操作系统，但对系统稳定性的极致追求使其无法频繁更新补丁。DCS 项目从软件定型到投运需经历漫长测试周期，微软每月发布的补丁无法及时部署，大量已知漏洞长期暴露。同时，为保障监控软件兼容性，

系统需开放 135、139、445 等高危端口，关闭将导致功能异常。防病毒软件部署同样两难：在线更新需连接外网，实时扫描可能影响控制任务实时性，大量操作员站长期“裸奔”。工程师站作为组态维护核心终端，频繁使用 U 盘进行程序下载和备份，成为恶意代码摆渡植入的主要载体。

2.3 管理制度与人员操作的薄弱环节

技术漏洞与人为因素叠加，使管理制度缺陷成为网络安全的重要放大器。账户管理上，多套 DCS 系统共用同一组管理员账号密码且长期不变、多人共用，发生误操作或恶意操作后无法溯源。权限管理粗放，绝大多数运维人员拥有工程师站全部操作权限，包括组态修改、下装、强制信号等高风险操作，过度授权增加误动和破坏概率。外包人员管理缺失，外部人员接触核心控制系统时缺少有效监督和审计[2]。两化融合深入后热工专业与信息专业交叉作业频繁但责任界面模糊，热工人员不懂网络、信息人员不懂工艺，网安管理“三不管”地带逐渐形成。

2.4 供应链安全与第三方集成的隐性风险

热工控制系统安全性不仅取决于系统集成商，更依赖供应链各环节的安全可控。从芯片、嵌入式操作系统、组态软件到通信模块，任何一层被植入恶意后门或存在未公开漏洞，均可能被攻击者利用。工程实施中大量第三方设备如智能变送器、执行机构、在线分析仪表通过现场总线接入 DCS，其固件安全水平参差不齐，部分不具备基本安全认证机制。系统改造扩容时不同厂家新旧设备混用，通信协议版本不一致，安全策略难以统一，引入大量未知风险。攻击者可通过供应链侧向渗透进入核心控制系统，这种攻击路径绕过所有外围边界防护，极具隐蔽性和破坏性。

3 热工控制系统网络安全防护对策

3.1 网络架构优化与区域隔离

基于“垂直分层、水平分区”的纵深防御思想，对热工控制系统网络架构进行安全重构。垂直方向将生产过程划分为控制区（安全区 I，含过程控制层和操作监控层）、非控制区（安全区 II，含生产管理应用）和外部信息区（办公网及互联网），各区之间通过电力专用横向单向隔离装置实现物理级隔离，确保管理网信息仅能单向传入监控网，控制指令绝不可能反向泄露。水平方向对同一区域内不同功能子系统（如锅炉侧、汽机侧、公用系统）进行 VLAN 逻辑隔离，缩小故障和攻击扩散半径。同时取消不必要跨区互联，对保留链路实施严格访问控制，仅开放业务必需的最小化端口和 IP 白名单，从根本上减少暴露面。

3.2 边界防护与入侵检测体系

在安全区域边界部署工业级防火墙和入侵检测系统，实现网络流量深度包解析与行为审计。工业防火墙应具备对 Modbus、DNP3、IEC 104 等工控协议的深度识别能力，解析应用层指令语义，对功能码、寄存器地址、设定值范围实施白名单策略——仅允许预设合法指令通过，异常指令即时告警并阻断。入侵检测系统采用特征匹配与异常行为分析双重机制，内置已知工控攻击特征库，同时通过学习正常工况流量基线，识别非工作时段大流量交互、异常协议组合、非授权 IP 控制指令等异常行为。所有边界设备日志统一采集至安全审计平台，实现安全事件的集中关联分析与可视化呈现。

3.3 主机系统加固与恶意代码防范

主机安全是热工控制系统防护的最后一道防线，须在保证控制功能正常前提下实施针对性加固。对操作员站、工程师站、历史服务器等核心主机实施最小化安装策略——卸载无关软件和服务，关闭非必需高危端口，禁用 USB 自动运行功能。账户管理采用双因素认证，结合 USB Key 和静态密码双重确认身份。权限管理遵循最小授权原则，按岗位划分为系统管理员、热工工程师、运行操作员三级，组态修改、下装、强制信号等高风险操作需二级审批并通过双人操作模式执行。恶意代码防范方面部署工业主机白名单防病毒软件，仅允许预先授权的可执行文件运行，未知程序自动拦截告警，从根本上阻断勒索软件感染，同时避免传统特征库升级带来的联网需求[3]。

3.4 纵深防御体系与应急响应机制

单一安全措施无法应对所有威胁，须构建“边界防护-主机加固-审计追溯-应急恢复”四层纵深防御体系。边界防护层通过防火墙和隔离装置拦截外部攻击；主机加固层通过系统安全配置和白名单机制阻断恶意代码执行；审计追溯层全范围开启操作系统和关键应用安全审计，记录所有用户操作行为（登录时间、执行命令、修改参数和组态文件等），确保攻击行为可发现、可追溯、可取证；应急恢复层制定网络安全专项应急预案，定期对工程师站和控制器组态进行离线备份，关键数据备份至安全离线存储介质，确保遭受勒索攻击或系统崩溃后能在最短时间内恢复至最近安全状态。每年至少组织一次网络安全应急演练，验证备份数据可用性和预案有效性。

3.5 全生命周期安全管理体系

网络安全不是一次性的技术部署，而是贯穿规划、设计、实施、运维到退役全生命周期的持续性管理活动。在规划设计阶段，将网络安全需求纳入系统总体设计，明确安全等级保护定级，预留安全设备的安装位置和网络接口，避免建成后“打补丁式”整改。在采购招标阶段，将网络安全功能要求写入技术规范书，明确要求供应商提供符合 IEC 62443 标准的设备和系统，并要求其提供完整的软件物料清单，便于后续漏洞跟踪。在施工调试阶段，严格控制外来设备和移动介质接入系统网络，调试完成后立即更改所有默认账户和密码，清理临时调试接口和测试程序，并完成首次全面的安全加固与漏洞扫描。在运维管理阶段，建立常态化的安全巡检制度，每月检查系统日志和审计记录，每季度对关键主机进行漏洞扫描，发现高危漏洞后组织专业评估并制定修补计划，在确认兼容性后通过离线补丁包方式实施更新。

4 典型攻击场景分析与防护验证

4.1 勒索软件感染场景及阻断路径

勒索软件入侵通常始于办公网终端或运维 U 盘，通过钓鱼邮件或供应链投毒进入管理信息网，利用防火墙开放的数据交换端口横向渗透至操作监控层，或通过感染 U 盘在工程师站完成摆渡。勒索软件执行后对历史数据库、组态工程文件、趋势归档等关键数据进行高强度加密，导致运行人员丧失参数调整、报警确认等高级监控功能[4]。阻断该场景的核心措施包括：在管理信息网与监控网之间部署单向隔离装置，切断横向渗透通道；在主机端部署应用白名单机制，禁止未授权可执行文件运行；对工程师站 USB 接口实施硬件管控，数据交换使用专用安全 U 盘并做到用前杀毒、专人专用。

4.2 内部恶意运维操作风险与控制

内部恶意运维操作虽不如外部攻击引人注目，但发生频率和实际破坏力往往更高。此类事件主体通常为具备工程师站高权限的运维人员，受经济利益或情绪驱动，在正常维护时段执行超出授权范围的危险操作，如擅自修改锅炉主控 PID 参数、强制复位保护信号、删除控制器组态文件等。由于操作者持有合法账户，传统防火墙和入侵检测设备完全无法识别和拦截。应对措施必须技术与制度协同：部署运维操作审计系统，对工程师站操作进行全程录屏与指令级记录，高风险操作需双人同时在场、各自刷卡确认方可执行；实行关键操作工单制度，控制修改权限与运行权限分离，外包人员作业须业主方全程陪同，操作完成后立即收回临时权限[5]。

结束语

热工控制系统网络安全关乎国家关键基础设施安全。本文从系统架构、通信协议、主机系统、管理制度及供应链安全等维度剖析了网络安全隐患，提出了网络架构优化、边界防护、主机加固、纵深防御体系及全生命周期安全管理等系统化对策，并针对勒索软件感染和内部恶意运维两类典型攻击场景分析了阻断路径。研究表明，热工控制系统安全防护不能照搬 IT 方案，须立足高可用性与高实时性要求，坚持安全与可用并重、管理与技术协同、静态防御与动态响应结合。唯有将安全理念融入系统全生命周期，构建多层次立体化纵深防御体系，方能在严峻威胁环境下确保系统安全稳定运行。

参考文献

[1] 邵新玉. 智慧电厂环境下热工控制系统信息安全防护策略研究 [J]. 工程技术研究,2026,8(5):13-15.

[2] 沈鹏. 电厂热工控制系统抗干扰技术研究 [J]. 现代制造技术与装备，2025，61(12):49-51.

[3] 黄思铭, 张玉珏, 袁豪杰. 工业控制系统网络安全态势感知平台设计 [J]. 软件，2024,45(2):95-97.

[4] 王海波. DCS 网络安全维护在电力系统监控中的关键技术研究与应用 [J]. 通信电源技术,2024,41(13):206-208.

[5] 莫小磊, 苗勇, 佟勇, 等. 工业控制系统勒索病毒分析及防护研究 [J]. 数字化转型,2025,2(2):75-85,98.